AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A computer-implemented process for receiving from a plurality of sending clients media packets across a firewall sent to a single destination address and a single destination port of a firewall, each media packet not including an unencrypted Synchronization Source Identifier (SSRC) but including an encrypted Synchronization Source Identifier, comprising the process actions of:

establishing a plurality of security associations (SAs) for dialogs between sending clients and receiving clients, each SA including source information of a sending client and an indication of a receiving client;

receiving from a sending client an encrypted media packet sent using Real-time Transport Protocol (RTP) message format at a media-relay server, the encrypted media packet being sent to the destination address and the destination port;

determining whether the sending client's Security Association (SA) exists using the sender's source information received with the media packet, the sender's source information being unencrypted and including a source address;

if no SA exists, dropping the media packet at the media-relay server; and

if a SA does exist, decrypting the media packet including decrypting a media packet Synchronization Source Identifier included in the media packet;

obtaining ~~a~~ obtained Synchronization Source Identifier ~~(SSRC)~~ from the SA;

comparing the media packet Synchronization Source Identifier included in the decrypted media packet with the obtained Synchronization Source Identifier obtained from the SA;

if the media packet Synchronization Source Identifier included in the decrypted packet does not match the obtained Synchronization

Source Identifier obtained from the SA, dropping the media packet; and

if the media packet Synchronization Source Identifier in the decrypted packet matches to the obtained Synchronization Source Identifier obtained from the SA, forwarding the packet to a receiving client indicated in the SA based on the sender's source information

wherein a plurality of sending clients send media packets with different encrypted Synchronization Source Identifiers to the destination address and the destination port.

2. (Original) The computer-implemented process of Claim 1 wherein the source information retrieved by the media-relay server comprises a source Internet Protocol (IP) address and port number found in the RTP message format.

3. (Original) The computer-implemented process of Claim 1 wherein the media packet comprises audio data.

4. (Original) The computer-implemented process of Claim 1 wherein the media packet comprises video data.

5-16. (Cancelled)

17. (Currently Amended) A method in a media-relay server for relaying to receiving clients packets of a real-time transport protocol received from sending clients through a single destination address and a single destination port of a firewall, each packet not including an unencrypted synchronization source identifier but including an encrypted synchronization source identifier, the method comprising:

for each of a plurality of sending clients, establishing a security association for a dialog between the sending client and a receiving client, the security

association including an encryption key for decrypting packets sent from the sending client to the receiving client via the destination address and the destination port, ~~a~~ an established synchronization source identifier that uniquely identifies the sending client within the dialog, source information of the sending client, and an indication of the receiving client;

receiving from a sending client a datagram of a user datagram protocol sent to the destination address and the destination port, the datagram including an encrypted packet and source information of the sending client, the source information of the sending client including a unencrypted source address; and

upon receiving the datagram,

when no security association has been established that includes the source information of the received datagram, dropping the encrypted packet; and

when a security association has been established that includes the source information of the received datagram,

decrypting the encrypted packet using the encryption key of the established security association including decrypting a packet synchronization source;

when the decrypted packet synchronization source ~~identifiers~~ identifier of the decrypted packet and the established synchronization source identifier of the established security association do not match, dropping the decrypted packet; and

when the decrypted packet synchronization source ~~identifiers~~ identifier of the decrypted packet and the established synchronization source identifier of the established security association do match, forwarding the decrypted packet to the

receiving client indicated in the established security association.

18. (Previously Presented) The method of claim 17 including receiving from each of the plurality of sending clients datagrams sent to the destination address and the destination port.

19. (Previously Presented) The method of claim 17 wherein the media-relay server is connected to a external firewall through which datagrams are received from sending clients and an internal firewall through which packets are forwarded to receiving clients.

20. (Previously Presented) The method of claim 17 wherein the source information is a source address and a source port of the datagram.

21-22. (Canceled)

23. (Currently Amended) A media-relay server for relaying to receiving clients packets of a real-time transport protocol received from sending clients through a single destination address and a single destination port of a firewall, each packet not including an unencrypted synchronization source identifier but including an encrypted synchronization source identifier, the media-relay server comprising:

security associations established for sending clients and receiving clients, the security association for a sending client including, ~~a~~ an established synchronization source identifier that uniquely identifies the sending client within the dialog, source information of the sending, and an indication of the receiving client;

a component that receives from a sending client an encrypted packet of the real-time transport protocol and source information of the sending client sent

by the sending client to the destination address and the destination port, the source information of the sending client including a unencrypted source address; and

a component that

when no security association has been established that includes the received source information, drops the encrypted packet; and

when a security association has been established that includes the received source information,

decrypts the encrypted packet including decrypting a packet synchronization source identifier included in the packet to a decrypted packet synchronization source identifier;

when a decrypted packet synchronization source identifier of the decrypted packet and ~~a~~ an established synchronization source identifier of the established security association do not match, drops the decrypted packet; and

when the decrypted packet synchronization source identifier of the decrypted packet and the established synchronization source identifier of the established security association do match, forwards the decrypted packet to the receiving client indicated in the established security association.

24. (Previously Presented) The media-relay server of claim 23 wherein packets are received from each of the plurality of sending clients sent to the destination address and the destination port.

25. (Previously Presented) The media-relay server of claim 23 wherein the media-relay server is connected to a external firewall through which encrypted packets are received from sending clients and an internal firewall through which decrypted packets are forwarded to receiving clients.

26. (Currently Amended) The media-relay server of claim 23 wherein the source information is a source address and a source port of the received packet ~~datagram~~.

27-28. (Canceled)